SANDIA REPORT
SAND2017-0794
Unlimited Release
Printed January 2017

Distributed Energy Systems: Security Implications of the Grid of the Future

Kevin L. Stamber, Andjelka Kelic, Robert A. Taylor, Jordan M. Henry, Jason E. Stamp

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2017-0794
Unlimited Release
Printed January 2017

Distributed Energy Systems: Security Implications of the Grid of the Future

Kevin L. Stamber
Systems Research, Analysis, & Applications
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1137

Andjelka Kelic
Robert A. Taylor
Policy & Decision Analytics
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1137

Jordan M. Henry
Critical Infrastructure Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0671

Jason E. Stamp
Special Cyber Initiatives
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0671

Abstract

Distributed Energy Resources (DER) are being added to the nation's electric grid, and as penetration of these resources increases, they have the potential to displace or offset large-scale, capital-intensive, centralized generation. Integration of DER into operation of the traditional electric grid requires automated operational control and communication of DER elements, from system measurement to control hardware and software, in conjunction with a utility's existing automated and human-directed control of other portions of the system. Implementation of DER technologies suggests a number of gaps from both a security and a policy perspective.

This page intentionally left blank.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

ARRA	American Reinvestment and Recovery Act
CPUC	California Public Utilities Commission
DER	distributed energy resources
DOE	Department of Energy
DSP	Distributed System Platform
EISA	Energy Independence and Security Act
FERC	Federal Energy Regulatory Commission
HTTP	hypertext transfer protocol
kW	kilowatt
MW	megawatt
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NYPSC	New York Public Service Commission
PUC	public utility commission
PURPA	Public Utility Regulatory Policies Act
RMP	Risk Management Plan
SNL	Sandia National Laboratories
VoIP	Voice over Internet Protocol

1. EXECUTIVE SUMMARY

Distributed Energy Resources (DER) are being added to the nation's electric grid, and as penetration of these resources increases, they have the potential to displace or offset large-scale, capital-intensive, centralized generation. Integration of DER into operation of the traditional electric grid requires automated operational control and communication of DER elements, from system measurement to control hardware and software, in conjunction with a utility's existing automated and human-directed control of other portions of the system.

The implementation of DER technologies suggests a number of gaps from both a security and a policy perspective. First, the convergence of information and communication technologies and electricity grid operations and control increase the potential attack surface of the power grid to malicious actors.

Second, authentication of information to and from DER devices (i.e., who can talk to a device) and integrity of those communications (determining that the information has not been modified in transit) are substantive issues and are essential to operational security.

Third, while a range of policy steps have been taken to accelerate additions of DER to the grid in the last two decades, similar policy steps to ensure cyber security of DER systems, and integration of DER systems with the larger grid, have lagged in comparison. This places the onus of identification and protection of critical cyber assets that control, or could impact, the reliability of bulk electric systems on a range of stakeholders, specifically balancing authorities, transmission operators, and reliability coordinators.

Fourth, at the state level, policy implementation has been mixed for securing DER systems, though this is to be expected. California was proactive, relative to Federal policies, by adding minimum cybersecurity requirements within the confines of existing regulatory rulemaking. On the other hand, in New York, state regulatory authorities deferred to NIST guidance, saying that "there is no single set of security standards that we can simply direct utilities to comply with. It is unlikely that any definitive set of standards will ever exist, given the threat."

Finally, a coordinated effort among stakeholders—the nation's utilities, state public utility commissions (PUCs), distributed-generation control hardware and software vendors, and communications providers—does not exist to address the growing attack surface. Grid operators are left to rely on the ability of DER operators at various scales, from large commercial entities to noncommercial users, to properly configure their networks. Congestion and network failures for commercial communications networks such as the Internet and the Public Switched Telephone Network, on which some elements of utility operational information may ride, can lead to an inability to properly communicate with distributed grid technology. Combined, these gaps create potential for distributed generation to have a negative effect on grid resilience.

This page intentionally left blank.

2. PROBLEM STATEMENT

Our national electric grid is evolving to include significant amounts of distributed generation, storage, and demand response, geared to lower the cost of electricity, increase energy security, reduce the environmental impact of energy production, and increase customer choice. Some distributed energy resource installations, such as those designed to provide power to a facility or area under emergency conditions in isolation from the larger grid, can increase systemic resilience at the local level. The evolution of grid architecture incorporating such resources will bring on new, as-yet unrealized security threats. These threats will be related to vulnerabilities of the system to natural events and human-caused malicious or accidental actions (whether cyber or physical). Several changes are driving this evolution of the grid, including the following:

- The integration of inverter-based systems, such as solar photovoltaics and storage technologies;
- Growth in connection of electric vehicles and associated charging stations;
- New controls and demand response technologies;
- The growing presence of Internet-connected grid devices; and
- The role of communications and commercial communications technologies and providers across widely distributed systems.

These technological changes in the structure of the electric grid are further influenced by economic and regulatory changes designed to accelerate the economic attractiveness of new technology options. It is not yet clear what all the security implications are of changing either the topological and functional structure of the electric grid or the control systems necessary to manage it, but technology development and policies are needed now that aim to ensure grid security as these issues evolve. The rate that regulation encourages market penetration of distributed generation has outpaced policy development supporting security and reliable communications implementation, creating several gaps.

This document addresses the evolving landscape in consumer-grid interactions and policy and explores gaps and paths forward to a more robust and secure grid. It begins by developing a picture of how Distributed Energy Resources (DER) are functionally being incorporated into the electric grid, describing the technologies involved and their potential risks. The document then discusses the technical, economic, and policy influences impacting the deployment and penetration of DER. Finally, the document identifies potential gaps in policy and research on security in DER deployments. Identifying and addressing these gaps will lead to a future grid that maintains reliability for consumers while enhancing environmental quality, increasing choices, lowering costs, and improving resilience of our energy infrastructure.

This page intentionally left blank.

3. THE EVOLUTION OF THE DISTRIBUTION SYSTEM (INCLUDING DISTRIBUTED ENERGY RESOURCES) AND THE IMPACTS ON SECURITY

Distributed Energy Resources date back to the world's earliest electrification projects where appropriately-sized power generation assets were placed close to load to meet demand. A combination of technological, economic, and regulatory effects has, in recent years, increased the deployment of distributed generation. Some of the technologies considered as part of distributed generation include small-scale fossil-fueled generation (e.g., reciprocating internal combustion engines, gas turbines, microturbines) and non-traditional generation, such as fuel cells, renewable energy assets like photovoltaic systems and wind turbines, along with storage devices, or combinations of these energy-producing technologies (El-Khattam, 2004). All of these technologies are designed to meet electricity demand closer to the point of consumption in significantly smaller increments than was traditionally done when adding capacity to the grid in more centralized locations.

For much of the last century, utilities, upon determining a need for additional generation to meet demand, would petition their state regulatory authority for permission to build additional generation, and would seek cost reimbursement from customers in the form of increased rates. The quantity of generation these utilities would build was based on long-term expectations of demand growth, and units would usually be in the hundreds of megawatts (MW) in capacity, either placed with existing generation of similar size, or in a new location. At the time, this was the most effective solution and would meet several years' worth of expected demand growth. Today, the attractiveness of distributed energy options is enhanced by the increased reliability of locally available generation. Along with wholesale energy available via competitive markets using open-access transmission, this serves as an additional option for utility planners in satisfying demand. DER sources installed by consumers, independent power providers, or other entities, are smaller, and require just a small installation footprint. Individual residential elements of a distributed generation solution can run as low as 5 kilowatts (kW) (El-Khattam, 2004), while combined facilities with multiple elements can be larger, into the MWs range, with states gradually increasing the lower bound of generation capacity that can be considered as DER, increasing the number of DER projects connected to the distribution system rather than to the transmission system (Powers, 2016).

Integration of distributed energy resources into operation with the traditional electric grid, particularly for microgrids designed to operate islanded from the primary grid in the event of disruption, requires automated operational control and communication of DER elements, from system measurement to control hardware and software, in conjunction with a utility's existing automated and human-directed control of other portions of the system. A range of power electronics devices (combinations of semiconductor switches, gating and control systems, inductive and capacitive components) are typically used for connecting distributed energy systems to the greater electric power system in distributed energy resource installations (Kroposki, 2010)(Colmenar-Santos, 2016). These devices provide the most potential for active, controlled integration with the grid. When integrated with energy demand management programs and technologies, these combined technologies significantly increase the attack surface of the national power grid and opportunity for risk to system operation from malicious actors.

In the US, states like Hawaii and California are good examples of increasing penetration of inverter-based distributed generation[1]. To address the increasing concern for cyber-secure distributed generation, the California Solar Initiative has put together several cyber security and testing recommendation documents related to residential inverter-based DER assets. Their recommendations specifically focus on communications modules that provide protocol conversion and the following communications pathways:

- From the utility to the device
- From the vendor to the device (for software updates, monitoring, diagnostics, or repair)
- From the aggregator (if there is an aggregator pulling all of the DER resources together) to the device (Henry, 2015)

Additionally, the following communications pathways are important in distributed generation:

- From the aggregator to the utility
- From the device to the utility

These communications pathways are shown in Figure 1. The cyber security and testing recommendations identified by the California Solar Initiative could be applied in that space as well.

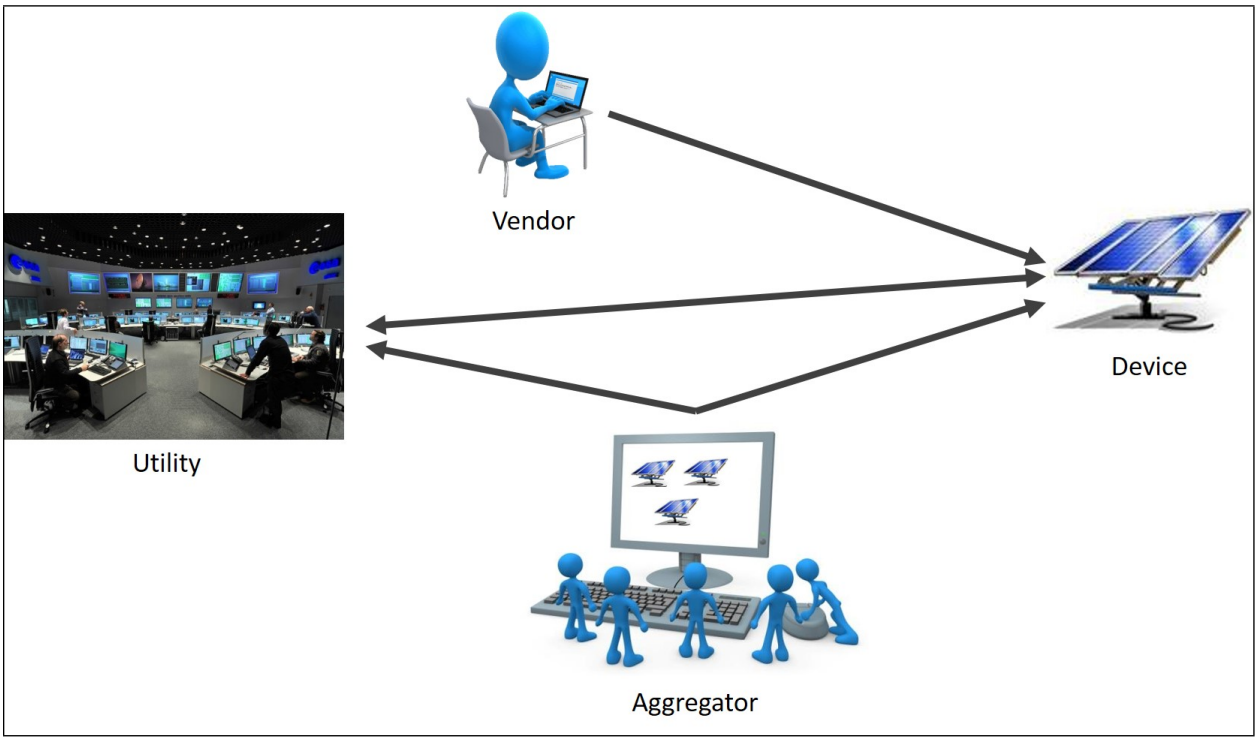

Figure 1. Communications Pathways Relevant to DER Integration, Operation, And Maintenance

[1] Inverter-based distributed generation includes fuel cells, wind turbines, solar photovoltaics, and microturbines reliant on inverters for interface to the electric grid (Keller & Kroposki, 2010), though solar photovoltaic sources dominate this category in terms of both net generation and number of metered installations.

Large utilities, both investor-owned and not-for-profit, use a range of methods for communications, often within the same utility, from utility-owned communications lines to microwave to the commercial telecommunications network. In residential and smaller commercial installations (as well as in large utilities), reliance on commercial telecommunications is present in grid control. For residential and small commercial installations, devices sit on a commercial internet service provider's network out of the control of the utility and any of its normal security mechanisms. This dependence on a commercial internet service provider's network puts the availability of DER resources network nearly exclusively under the control of the commercial internet service provider, and may place system security in the hands of the consumer who may have any number of additional devices on their home or business network with varying levels of security in place. It also represents an increase in the potential cyber-attack surface. This, naturally, raises the potential for questions as to how security will be adequately established, given the diverse nature of these networks.

Availability of an intermittently used device, such as a DER reliant on the sun or wind, is less critical than for an always-on device, since a utility system is already designed to accommodate the uncertainty associated with the device's operation (Henry, 2015). However, authentication (answers the question, Who can talk to the device?) and integrity (answers the question, Has the information been modified in transit?) are discussed as much larger issues, and are essential to operational security.

A range of theoretical attacks against the communications architecture-supporting utility and DER operations are possible. For example, an intruder could create a denial-of-service attack so that control commands could not reach the DER, or leverage other security vulnerabilities on the consumer network to intercept control and monitoring traffic and potentially modify it in transit, or even to compromise the DER devices themselves. Weaknesses and vulnerabilities of this nature have been regularly identified and presented both in print and at hacker conferences like DEFCON. In one case, a homeowner identified multiple risks to his household solar array's control system, including an open wireless access point and services provided over an unencrypted hypertext transfer protocol (HTTP) connection, allowing for a brute-force attack to guess at the system's username and password (Fox-Brewster, 2016). Similarly, German researcher Maxim Rupp identified flaws in large-scale wind turbine and solar array control systems requiring a low level of skill to exploit and that could be used to turn off power supplies using the control systems (Fox-Brewster T. , 2015). Producing effective attacks on the DER devices may require reverse engineering and detailed knowledge and tools related to gaining access and control of the device itself. Most DER controllers are embedded systems running firmware that is specific to that controller. As such, the majority of attacks leverage vulnerabilities on the network side of the device. Nevertheless, it stands to reason that increased advanced communication and control of distributed generation assets could have implications on the power grid, both at a local and regional level (if enough distributed generation is exposed and subverted).

This page intentionally left blank.

4. POLICIES INFLUENCING TECHNOLOGY IMPLEMENTATION AND SECURITY

A variety of technical, economic, and policy influences affect the adoption and implementation of distributed generation technologies (Colmenar-Santos, 2016). There are several positive aspects from a technical perspective. Siting generation closer to demand reduces losses in the movement of power, which are correlated with the distance required for power to travel to meet system load. The availability of distributed generation as a supplement to traditional supply of electric power can also improve the quality of power used by eliminating voltage sags and improving consumer reliability.

From an economic perspective, a combination of technology improvements and large-scale capital investments have led to dramatic reductions in the cost per unit of power generated for various distributed energy resources. This is especially true for photovoltaics and wind energy, with the cost of energy of onshore wind in Europe dropping 65% between 1988 and 2014 (International Renewable Energy Agency, 2015), and the cost of solar cells dropping by 65% between 2009 and 2013 (International Renewable Energy Agency, 2014), with continued cost declines over the next decade expected (International Renewable Energy Agency, 2016). Economics of implementation of these technologies were also enhanced by financial incentives at the local and state level. In the past several years, various state and local governments have employed a number of financial incentive programs such as loans, direct rebates, tax credits, and feed-in tariffs to drive the development of renewable electricity production capacity. Specific examples are presented as part of the Appendix for selected states (Hawaii, California, Vermont, and New York). Although the direct effectiveness of individual programs is beyond the scope of this analysis, available net metering production capacity and advance meter adoption data (see Table 1) reveal the overall trend toward the smart grid posture in each of our target states.

Table 1. Growth in Wind and Photovoltaic Capacity for Selected States*

State	Year	Residential Photovoltaic Capacity (MW)	Commercial Photovoltaic Capacity (MW)	Industrial Photovoltaic Capacity (MW)	Total Photovoltaic Capacity (MW)	Total Number of Meters - Photovoltaic	Residential Wind Capacity (MW)	Commercial Wind Capacity (MW)	Industrial Wind Capacity (MW)	Total Wind Capacity (MW)	Total Number of Meters - Wind
Hawaii	2012	84.8	36.3	-	121.1	22,264	0.1	0.1	-	0.2	35
	2013	173.2	47.4	-	220.6	40,511	0.1	0.2	-	0.3	38
	2014	230.9	60.2	-	291.1	51,895	0.1	0.2	-	0.3	40
California	2012	734.3	525.0	277.4	1,536.7	158,940	3.7	1.6	7.1	12.4	481
	2013	1,054.3	577.3	409.3	2,040.9	233,181	3.6	2.1	7.0	12.7	567
	2014	1,592.6	705.5	493.5	2,791.6	337,099	3.6	2.2	8.0	13.7	568
Vermont	2012	14.9	3.8	0.2	18.9	2,316	0.4	0.1	-	0.5	62
	2013	15.2	4.5	0.2	19.9	2,676	0.5	0.1	-	0.6	58
	2014	23.9	7.5	0.2	31.6	3,895	0.5	0.2	-	0.7	68
New York	2012	50.7	47.5	0.1	98.3	10,785	0.8	0.6	-	1.4	138
	2013	83.8	89.6	2.2	175.6	15,826	2.3	1.2	0.2	3.6	305
	2014	165.3	143.6	3.7	312.7	29,175	2.4	2.4	0.2	4.9	322

**Note the order of magnitude of difference between photovoltaic installations, both in terms of capacity and number of meters, relative to wind installations for the states examined.*

For example, in terms of total install capacity, California has the largest installed distributed photovoltaic capacity of the four states considered in this discussion. In 2014 (most recent available data), California has approximately 2,800 MW of distributed photovoltaic production capacity installed. In this same year, California achieved a capacity allocation among its

residential, commercial, and industrial sectors of 57 percent, 25 percent, and 18 percent, respectively. New York in this same year achieved an allocation of 53 percent residential and 46 percent commercial, with a total installed capacity of 313 MW. By comparison, both Hawaii and Vermont achieved relatively high allocations of their distributed photovoltaic production capacity in their residential sectors. In 2014, almost 80 percent of Hawaii's capacity was installed in its residential sector with a total installed capacity of 291 MW. Likewise, Vermont had 76 percent of its 32 MW allocated in its residential sector. Table 1 shows capacity (in MW) and number of meters for photovoltaic and wind systems for each of the four states.

From the formal policy development standpoint, 2007 was a pivotal year, with the enactment of the Energy Independence and Security Act (EISA) (P.L. 110-140). Title XIII of EISA (Government Printing Office, 2007) established grid modernization through maintenance of a reliable and secure electricity infrastructure as a national policy. Under Title XIII of EISA, the director of the National Institute of Standards and Technology (NIST) was given primary responsibility for coordinating development of a framework for interoperability of grid devices and systems. Language in EISA also amended the Public Utility Regulatory Policies Act of 1978 (PURPA) to allow state utility regulatory authorities to amend their policies on grid investments to consider requiring inclusion of smart grid investments.

In the years that followed, a concerted effort was made on the part of federal regulatory bodies and standards organizations to promulgate the rules and guidelines to move the grid modernization vision presented by Congress forward. To provide the seed funding for the grid modernization vision, the American Reinvestment and Recovery Act (ARRA) (P.L. 111-5) appropriated $4.5 billion for Title XIII grid modernization projects in 2009. During the period of 2007 through 2014 there was a series of policy actions in the grid security space that set the ground rules for state-level action. For example, in 2012, the U.S. Department of Energy (DOE), in collaboration with NIST, the North American Electric Reliability Corporation (NERC), and with input from members of industry, developed the electricity subsector cybersecurity Risk Management Plan (RMP) Guideline (Edison Electric Institute, 2014) (US Department of Energy, 2012). Two years later NIST released its Cybersecurity Framework Version 1.0. This framework was designed to offer organizations, regulators, and consumers a cost-effective approach to manage cyber risk across the nation's critical sectors (US Department of Energy, 2014) (NIST, 2014).

The development of state-level policies related to grid modernization reflect the logical progression from national-level policy mandates and controls to specific technology implementation by utilities in compliance with federal and subsequent state-level policies. With the bulk of the initial work to establish national-level policy controls for grid modernization largely completed by 2013, state legislatures began taking action around this time (or slightly before) to formalize state policy on grid modernization.

There are distinct pros and cons to defining compliance-based security regulatory policies relative to nascent, maturing technologies such as DER systems and components, as opposed to security-based standards. Such compliance-based policies cannot be defined before the technology exists, and often has to be delayed until not only the individual components of the technology are mature, but until systems designed to control said components have been

developed and are matured. Within this development window, and in the absence of regulation, industry-defined best practices designed to minimize systemic risk, geared around a security basis, are essential to be followed. The legal risk of deploying technology with security flaws can be significant and threaten the economic well-being of nascent technology developers.

In general, the resulting legislation established paths to the integration of DER for the state and directed public utility commissions (PUCs) to begin formulating operational regulation requirements for the states' utilities. The degree to which these state-level actions incorporated specifics regarding security for DER integration varied substantially. For example, in 2011, New York passed legislation establishing a state-wide smart grid policy. This legislation allowed for two-way digital communication between electric utilities, their distribution grid and customers. This legislation aimed to improve efficiency and reliability of the electrical distribution system, while decreasing electric prices throughout the state, and providing increased protection of the state's electric grid through remote monitoring of critical infrastructure and key assets (EIA, 2011). New York's legislation, however, lacked any reference to security policies for implementation of the systems permitted. In that same year, the New York Public Service Commission (NYPSC) approved a policy statement establishing smart electric grid guidelines for utilities and grid modernization in general (NGA, 2015).

The conversion of law into enabled policy at the PUC level expresses the need for security, but also shows the limitations of the conversation. In their 2015 order on *Reforming the Energy Vision* (State of New York Public Service Commission, 2015), the NYPSC identified a number of potential issues in a reformed electric system with utilities acting as Distributed System Platform (DSP) providers. Among these issues was security. The NYPSC recommended following the technical guidance for smart grid cyber security assembled by NIST as a primary reference, saying that "there is no single set of security standards that we can simply direct utilities to comply with. It is unlikely that any definitive set of standards will ever exist, given the threat." The NYPSC did not direct the adoption or development of a specific set of cyber security standards as part of this order (State of New York Public Service Commission, 2015).

Some of the state's utilities, in comment on proposed regulation of DER products and services, proposed adding a new section to address cybersecurity concerns. These utilities suggested "at a minimum, the agreements shall include a requirement for all DERs and ESCOs to document and implement a cyber security policy that represents a commitment to appropriate cyber security protections, aligned with the National Institute of Standards and Technology Cyber Security Framework as applicable to the entity's business." The utilities involved preferred that DERs would have compliance-based processes and procedures in place, especially protocols for addressing and documenting breaches, and requirements for cybersecurity insurance (Joint Utilities, 2015). While protocols for addressing and documenting breaches are straightforward, requirements for insurance could create high hurdles to market entry for many DER market participants, as the costs would be distributed over a much smaller revenue base than the typical investor-owned utility.

In contrast, California was substantially more aggressive adding DER security to the existing regulatory code structure. Beginning in 2011, the California Public Utilities Commission (CPUC) began creating standards for data access and privacy in order to provide clear direction

on customer data ownership and access (CPUC, 2011). The California Energy Commission and the CPUC drafted a series of cybersecurity and privacy requirements under Electric Rule 21, the tariff that describes interconnection, operation, and metering requirements for connection of generation facilities to the distribution system. Recommendations for cybersecurity included a range of basic cybersecurity requirements (e.g., end-to-end requirements, implementation validation before data is exchanged, and a minimum of authentication, authorization, accountability, and data integrity). Privacy policies are also to be clearly defined (CPUC, 2015).

Once the states established PUC policy controls, work on funding pilot projects to deploy smart grid concepts began. In California, for example, two smart grid development projects (one led by San Diego Gas & Electric, the other by Bosch and American Honda) were documented in 2015 alone. Similarly, in New York four grid modernization projects were documented in 2014 and 2015 (NGA, 2015). These and other policy and regulatory actions are summarized in the Appendix to this document. It is important to note that while some of the policies identified in the Appendix, along with those outlined in one reference (Henry, 2015), have a cybersecurity focus, many regulatory policy examples at the state level, where PUC regulation of distribution companies (where most distributed generation is connected) is focused more on improving market penetration of distributed generation technologies, with a lighter emphasis on doing so with the above-mentioned security policies in mind.

Finally, with technical implementation uncertainty decreasing, states are beginning to issue more aggressive renewable energy portfolio standards. The most dramatic example of this can be found in Hawaii where, in 2015, a target of 100% of electricity that must be derived from renewable resources by 2045 was set.

5. GAPS IN POLICY AND RESEARCH REGARDING DISTRIBUTION GRID SECURITY

There are several potential gaps in grid security for distributed generation that deserve further examination, namely:

- The lack of a lock-step rollout of policies favoring DER market penetration and policies defining sound and complete security management of DER systems;
- The risk associated with DER systems being connected to local networks with existing security vulnerabilities;
- The reliance of DER systems on commercial communications networks;
- The gap between where regulation of DER systems is focused (at the bulk electric system level) and where the majority of those systems are connected (at the distribution level); and
- The opportunity for disruption of DER resources due to the disruption of other infrastructures.

This section will discuss these gaps in more detail. First, there is an incentives-based push to install renewable generation, which can be used in turn as a component of a DER implementation, reflected in tax and other incentives provided to purchasers of said technology. When combined with reduction in the cost of wind and photovoltaic technology, this creates a driver for DER technology market penetration. This push to create market penetration for distributed grid technology outpaces security and communications reliability implementations necessary to make these systems run effectively in concert with the larger electric grid. This imbalance between market penetration and security creates several opportunities for other problems.

Placing distributed generation technologies on consumer communications networks (e.g., business or residential networks) increases the attack surface available to malicious actors. While the potential consequences to this additional attack surface may be small for any individual malicious action, the business risk to DER of such an action, and its impact on future and planned deployments, must be considered and weighed on both DER companies and utilities reliant on DER for satisfying demand. Distributed generation technologies share the network with other equipment in the home or business, such as computers or "Internet of Things"[2] devices which have their own security vulnerabilities. The elements of distributed generation are therefore reliant on the home users' ability to properly configure and secure their own networks.

Coupling this with reliance on commercial communications providers (e.g., internet service providers) who may not have sufficient reliability standards needed by the electric grid due to any number of factors (e.g., network failures, congestion) could lead to reliability issues at the distribution level, the precise area DER implementation is meant to improve reliability.

[2] The "Internet of Things" is an internetworking of devices embedded with electronics, software, sensors, and network connectivity designed to allow for the collection and exchange of data between said devices. In the home, this includes programmable and learning thermostats, internet-connected refrigerators, and many other "smart" devices. In addition to home networking, applications also exist in manufacturing, energy management, and healthcare.

To date, federal policies and standards (NERC, 2016) (FERC, 2008) have focused heavily on the adoption of smart grid and DER technologies and security of the bulk power grid. However, DER technologies are often connected to the grid at the distribution level. This leaves a potential gap in the interpretation of federal standards and their applicability to many DER resources. The policies as defined place the onus of identification and protection of critical cyber assets that control or could impact the reliability of bulk electric systems on balancing authorities, transmission operators, and reliability coordinators. Many DER assets might at best operate in conjunction with a distribution operator that also happens to be a transmission operator. Security efforts have been directly related to DER and DER-controlled technologies and associated modes of communications (for example, security of information in transmission over a wireless network, or authentication of communications between end points). From a security management perspective, information security associated with communications for any purpose relies on three components. They are the following:

- Confidentiality, or measures taken to ensure that sensitive information is not seen by the wrong people, while making certain that those who should have access to sensitive information can get to it;
- Integrity, which is an assurance that the information is consistent, accurate, and trustworthy to all those authorized to access, and that data cannot be altered by those unauthorized to do so; and
- Availability, or reliable access to information by those authorized (ISRMC, 2009).

In terms of information security, existing security efforts conducted in the integration of DER technologies have led to a focus on the confidentiality and integrity of DER communications, but very little effort exists around availability. Aside from anecdotal comments related to DER and smart technologies existing potentially on a home user's network (Ghansah, 2012), the topic receives little attention. The availability aspect of information security is a gap in the existing policies related to security in the DER space. As these resources are pushed further to the edge of the distribution network, they are also moved outside of the communications links of the electric utility's own control system networks. Rather than sitting on a utility-owned network where that utility can have some control over reliability and availability (recognizing that some links in the current control network are acquired from commercial communications carriers), these new links sit firmly within a commercial communications carrier's network. From the electric utility's perspective, services provided by a commercial communications carrier are not guaranteed from a reliability and availability perspective.

DER technologies connect to one another and back to the utility through commercial communications assets that are on the electrical distribution network. In many cases, due to telecommunications regulations, these commercial communications assets are required to have backup power for some amount of time in the event of an electrical outage. When an electric utility is prioritizing restoration among customers, the presence of backup generation (as in this case) leads to assets being lower on the restoration list. The presence of backup generation also leads communications asset owners/operators to not purchase restoration priority from their local electric utility. In shorter duration outages, this is not an issue. However, in a longer outage, prioritization of fuel for backup power generators becomes a constraint on continuous operation of communications assets. This is driven by the fact that other infrastructure assets (e.g.,

hospitals, interstate pipeline pumps, water treatment plants) will receive higher priority than these communications assets for backup generator fuel, and, as a result, may cease to operate when fuel runs out, causing any dependent DER system to lose contact with the control network. As a result, the ability of a distribution utility to rely on DER resources as part of their restoration strategy is debatable at best. A thorough re-examination of electric grid restoration priorities, in light of these dependencies, may yield valuable insights for maintaining grid reliability during outage and restoration events, and deserves further study.

Commercial communications carriers use prioritization of traffic within their own networks to guarantee reliable service for voice communications carried over Voice over Internet Protocol (VoIP). These communications compete with all other traffic on the network, such as video streaming, so prioritization of service is required to ensure reliability. Regulations related to voice service reliability drove these decisions by the commercial carriers, but the technique could also be applied to control traffic for an element of distributed generation if the appropriate agreements could be reached between the electric power utility and the communications carrier. All of these elements are potential opportunities for failures of the grid due to disruption of other dependent infrastructures not experienced by the traditional electric grid, and they are not covered in current security discussion or regulations.

This page intentionally left blank.

6. CONCLUSIONS

Integration of distributed generation technologies for more flexible operation of the electric grid has become a part of the vision of policy makers since the early days of electric utility deregulation. Technology improvements have been made to make these technologies cost-effective for individual consumers, accelerating the deployment and penetration of a range of technologies. Consumer-side incentives have served to increase that penetration. Communication with distributed energy resources is essential for integrating their performance into the larger electric grid, even if the perspective of that communication is constrained to a particular distribution company among the thousands of distribution companies across the country to which resources may be connected. Authentication of communications and integrity of information flows are essential.

But policy implementation encouraging market penetration of distributed generation has outpaced policy development supporting security and reliable communications implementation, and this has created several gaps. In the absence of coordinated effort among the nation's utilities, state PUCs, distributed generation control hardware and software vendors, and communications providers on which communications between distributed generation and controlling entities (utilities or aggregators) rely, the potential attack surface of the power grid to malicious actors has increased. Grid operators are left to rely on the ability of noncommercial users to properly configure their networks. Congestion and network failures for commercial communications networks can lead to an inability to properly communicate with distributed grid technology. Combined, these gaps create potential for distributed generation to have a negative effect on the grid.

This page intentionally left blank.

7. REFERENCES

CERT. 2003. *The National Strategy to Secure Cyberspace.* Washington: US CERT. Accessed August 2016. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Colmenar-Santos, A., C. Reino-Rio, D. Borge-Diez, and E. Collado-Fernandez. 2016. "Distributed generation: A review of factors that can contribute most to achieve a scenario of DG units embedded in the new distribution networks." *Renewable and Sustainable Energy Reviews* 1130-1148.

CPUC. 2012. *Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission.* Sacramento: CPUC, 32.

CPUC. 2015. *Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters.* Sacramento: California Energy Commission and California Public Utilities Commission.

DHS. 2003. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.* https://www.dhs.gov/homeland-security-presidential-directive-7.

—. 2016. *National Cybersecurity and Communications Integration Center Description.* Accessed August 2016. https://www.dhs.gov/national-cybersecurity-and-communications-integration-cente.

DOE. 2015. "Los Angeles Department of Water and Power Smary Grid Regional Demonstration Program." *US Department of Energy Office of Electricity Delivery and Energy Reliability.* September. Accessed August 2016. https://www.smartgrid.gov/files/OE0000192_LADWP_FactSheet.pdf.

DOE. 2009. *National SCADA Test Bed Fact Sheet.* Washington, DC, September 16. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf.

DPS, Vermont. 2016. "2016 Vermont Comprehensive Energy Plan." *State of Vermont Department of Public Service.* Accessed August 2016. http://publicservice.vermont.gov/sites/dps/files/documents/Pubs_Plans_Reports/State_Plans/Comp_Energy_Plan/2015/2016CEP_ES_Final.pdf.

Eber, Kevin. 2016. *To Protect the Grid from Hackers, You Need to Break It.* June 7. Accessed August 2016. http://energy.gov/articles/protect-grid-hackers-you-need-break-it.

Edison Electric Institute. 2014. "Electric Power Industry Initiatives To Protect The Nation's Grid From Cyber Threats." *Edison Electric Institute.* October. Accessed August 2016. http://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Cybersecurity%20Backgrounder.pdf.

EIA. 2011. "Smart Grid Legislative and Regulatory Policies and Case Studies." *Energy Information Administration.* Accessed August 2016. https://www.eia.gov/analysis/studies/electricity/pdf/smartggrid.pdf.

—. 2016. *State Profiles and Energy Estimates.* Accessed August 2016. http://www.eia.gov/state/.

El-Khattam, W., and M.M.A. Salama. 2004. "Distributed generation technologies, definitions, and benefits." *Electric Power Systems Research 71 (2)* 119-128.

Energetics. 2006. *Roadmap to Secure Control Systems in the Energy Sector.* Washington: US Department of Energy. Accessed August 2016. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf.

Energy Information Administration. 2011. *Smart Grid Legislative and Regulatory Policies and Case Studies.* Washington: US Department of Energy. Accessed August 2016. https://www.eia.gov/analysis/studies/electricity/pdf/smartggrid.pdf.

Energy Sector Control Systems Working Group. 2011. *Roadmap to Achieve Energy Delivery Systems Cybersecurity.* Washington: US Department of Emergy. Accessed August 2016. http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

EPRI. 2006. *Compliance Guidelines for Cyber Security Reliability Standards - 2006 Update.* Palo Alto: Electric Power Research Institute. Accessed August 2016. http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001013301.

Erlin, Tim. 2016. "Hello There, NERC CIPv6." *Tripwire*, February 1. https://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip/hello-there-nerc-cipv6/.

Federal Energy Regulatory Commission. 2012. *Assessment of Demand Response and Advance Metering: Staff Report.* Washington: Federal Energy Regulatory Commission. Accessed August 2016. http://www.ferc.gov/legal/staff-reports/12-20-12-demand-response.pdf.

FERC. 2008. "18 CFR Part 40, Mandatory Reliability Standards for Critical Infrastructure Protection." *Federal Energy Regulatory Commission.* January 18. Accessed August 2016. http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf.

Fox-Brewster, T. 2016. "This Man Hacked His Own Solar Panels... And Claims 1,000 More Homes Vulnerable." *Forbes*, August 1. Accessed August 2016. http://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers/#441b2fef3811.

Fox-Brewster, Thomas. 2015. "Hundreds of Wind Turbines and Solar Systems Wide Open to Easy Exploits." *Forbes*, June 12. http://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar-systems-is-easy/#133c246e27a6.

Ghansah, Isaac. 2012. *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks.* Sacramento: California Energy Commission, PIER Energy-Related Environmental Research Program. Accessed August 2016. http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf.

Government Printing Office. 2007. *P.L. 110-140, Energy Independence and Security Act (EISA) of 2007.* Washington, DC: Government Printing Office. Accessed August 2016. https://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf.

Henry, J., R. Ramirez, F. Cleveland, A. Lee, B. Seal, T. Tansy, B. Fox, and A. Pochiraju. 2015. *Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications.* Sacramento: California Public Utilities Commission. Accessed August 2016. http://calsolarresearch.ca.gov/images/stories/documents/Sol4_funded_proj_docs/EPRI4_Seal/CSI_RDD_EPRI-Seal_Sol4_CyberSecurity.pdf.

International Renewable Energy Agency. 2016. "Average Costs for Solar and Wind Electricity Could Fall 59% by 2025." *International Renewable Energy Agency press release.* June 15. http://www.irena.org/News/Description.aspx?NType=A&mnu=cat&PriMenuID=16&CatID=84&News_ID=1452.

International Renewable Energy Agency. 2015. *Renewable Power Generation Costs in 2014.* Abu Dhabi: International Renewable Energy Agency. Accessed August 2016. http://www.irena.org/menu/index.aspx?mnu=Subcat&PriMenuID=36&CatID=141&SubcatID=494.

International Renewable Energy Agency. 2014. *REthinking Energy: Towards a new power system.* Abu Dhabi: International Renewable Energy Agency. Accessed August 2016. http://www.irena.org/rethinking/default2014.aspx.

ISRMC. 2009. *Confidentiality, Integrity & Availability.* http://ishandbook.bsewall.com/risk/Methodology/CIA.html.

Joint Utilities. 2015. *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products: Initial Commments of the Joint Utilities to the Notice Seeking Comments on Proposed Standards.* Albany: State of New York. Accessed August 2016. http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={43ED92A1-AEAA-4E5A-A2C2-9082FE2A1B7E}.

Keller, J, and B Kroposki. 2010. *Understanding Fault Characteristics of Inverter-Based Distributed Energy Resources.* Golden: National Renewable Energy Laboratory. Accessed December 12, 2016. http://www.nrel.gov/docs/fy10osti/46698.pdf.

Keogh, Miles. 2009. *The Smart Grid: Frequently Asked questions for State Comissions.* National Association of Regulatory Utility Commissioners. Accessed August 2016. http://pubs.naruc.org/pub/539D0510-2354-D714-5127-EAEE53F3D405.

Kroposki, B., C. Pink, R. DeBlasio, H. Thomas, M. Simoes, and P. K. Sen. 2010. "Benefits of Power Electronic Interface for Distributed Energy Systems." *IEEE Transactions on Energy Conversion* 901-908.

NCCETC. 2016. *Database of State Incentives for Renewables & Efficiency (DSIRE).* Accessed August 2016. http://www.dsireusa.org/.

NERC. 2016. *CIP Standards.* Accessed August 2016. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

—. 2015. *CIP V5 Transition Program.* Accessed August 2016. http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx.

—. 2016. *Program Areas & Departments > Standards > 1200 - Cyber Security (Urgent Action).* Accessed August 2016. http://www.nerc.com/pa/Stand/Pages/1200Cyber_Sec_Renewa.aspx.

NGA. 2014. "Governors' Guide to Modernizing the Electric Power Grid." *National Governors Association.* Accessed August 2016. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf.

—. 2015. *State Clean Energy Acxtions Database.* Accessed August 2016. http://www.nga.org/cms/cleanenergysearch.

—. 2014. "State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure." *National Governors Association.* Accessed August 2016. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1408EnhancingCybersecurityEnergySystems.pdf.

NIST. 2014. *NIST Releases Cybersecurity Framework Version 1.0.* February 12. Accessed August 2016. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development System. 2011. D.11-07-056 (California Public Utilities Commission, July 29).

PCCIP. 1997. "Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Criitcal Infrastructure Protection." Washington. Accessed August 2016. https://www.fas.org/sgp/library/pccip.pdf.

Powers, Mary. 2016. *New York increases allowable distributed geenration projects to 5 MW.* March 21. Accessed August 2016. http://www.platts.com/latest-news/electric-power/birmingham-alabama/new-york-increases-allowable-distributed-generation-26401515.

RTA Automation. 2016. *MODBUS RTU.* Accessed August 2016. http://www.rtaautomation.com/technologies/modbus-rtu/.

SDG&E. 2015. "SDG&E Receives $5 Million Grant to Expand Borrego Springs Microgrid." *San Diego Gas & Electric.* February 17. Accessed August 2016. http://www.sdge.com/newsroom/press-releases/2015-02-17/sdge-receives-5-million-grant-expand-borrego-springs-microgrid.

SGIP. 2010. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security.* Smart Grid Interoperability Panel. Accessed August 2016. https://www.smartgrid.gov/files/nistir_7628_.pdf.

State of Hawaii. 2016. *Hawaii Clean Energy Initiative.* Accessed August 2016. http://www.hawaiicleanenergyinitiative.org/.

State of New York Public Service Commission. 2015. *Case 14-M-0101 - Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision: Order Adopting Regulatory Policy Framework and Implementation Plan.* Albany: State of New York. Accessed August 2016. http://energystorage.org/system/files/resources/0b599d87-445b-4197-9815-24c27623a6a0_2.pdf.

Symantec. 2008. *Control Compliance Suite - NERC and FERC Regulation.* Cupertino, CA. Accessed August 2016. http://eval.symantec.com/mktginfo/enterprise/fact_sheets/b-datasheet_css_nerc_ferc.10-2008.14566044-1.en-us.pdf.

US Department of Energy. 2014. *2014 Smart Grid System Report: Report to Congress, August 2014.* Washington: US Department of Energy. Accessed August 2016. http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf.

US Department of Energy. 2012. *Electricity Subsector Cybersecurity Risk Management Process.* Washington: US Department of Energy. Accessed August 2016. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

This page intentionally left blank.

APPENDIX A: SURVEY OF REGULATORY AND POLICY ACTIONS REGARDING DISTRIBUTED GENERATION IMPLEMENTATION AND INCENTIVIZATION, INCLUDING GRID SECURITY

Introduction

In this section, we conduct a review of energy policy actions over the past 10 years at the federal and state level to better understand the state of policy development in the area of distributed generation security. First, Federal policies that most closely relate to smart grid security issues are summarized in chronological order. Second, for the state level perspective, we focus on 4 states: Hawaii, California, Vermont, and New York. For each state, energy policies and actions that most closely relate to distributed generation issues are summarized in chronological order. It's important to note that the lists of federal and state policies presented here are not exhaustive but represent a sample of the type of policies and actions found. In this initial version of this analysis, the goal is to get an overall sense of the evolution of policy from the federal down to the state level over the 10 years considered. With this review in hand, we can then begin to intuit the overall strengths and emphasis of the current grid security policy regime and look for areas where additional emphasis may be warranted.

Review of Distributed Generation Policies and Actions

It is clear from this initial review of distributed generation policies and actions that grid security is an increasing priority for both the public and private sector, but that much of the actions taken are at the federal level. The following policy compilation represents a first pass review of material covering the past decade related to this issue. Additional information and examples will be added as they become available.

National Level Policies and Actions

1997 – President's Commission on Critical Infrastructure Protection – the PCCIP laid the groundwork for defining the risk to the function of critical infrastructure, including electric power, from information-based attacks. "The widespread and increasing use of SCADA systems for control of energy systems", it reported, "provides increasing ability to cause serious damage and disruption by cyber means." The report strongly recommended a partnership between the public and private sectors in securing systems (PCCIP, 1997).

2003 – The National Strategy to Secure Cyberspace – This document reiterated the risks identified in (PCCIP, 1997) and discussed the government's role in light of the establishment of the Department of Homeland Security. The document articulated a series of priorities, and a series of actions and initiatives for meeting these priorities (CERT, 2003).

2003 (renewals in 2004 and 2005) - NERC Standard 1200 – Urgent Action Cyber Security Standard - The intent of the NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America (initially, control areas; in later iterations, balancing authorities, transmission operators, and reliability

coordinators) identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems (NERC, 2016).

2003 – Homeland Security Presidential Directive 7 (HSPD-7) – HSPD-7 designated sector-specific agencies (SSAs) for each of the nation's critical infrastructure sectors, stating that those agencies shall collaborate with relevant Federal, State, and local governments, and with the private sector; conduct or support vulnerability assessments; and encourage mitigation of risk through sound risk management strategies. The Department of Energy was identified as the SSA for the energy sector, including electric power (DHS, 2003).

2003 – National SCADA Test Bed (NSTB) – The DOE Office of Electricity Delivery and Energy Reliability established the NSTB to enable hardware and software vendors to test and assess vulnerabilities on a common platform, with resources at Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory, and Oak Ridge National Laboratory. This effort has led to the testing of most current SCADA market offerings, security training of hundreds of asset owners, and definition of best practices, among other benefits (DOE, 2009).

2004 - NERC Standard 1300 - Cyber Security - NERC Cyber Security is based on CIP-002 through CIP-011. Its goal is to prevent cyber threats and protect critical cyber assets that can affect the reliability of bulk electric system. The CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets (Symantec, 2008) (NERC, 2016). NERC Cyber Security Standards were submitted to FERC in August 2006 and approved by FERC in January 2008 (FERC, 2008).

2006 - Compliance Guidelines for Cyber Security Reliability Standards - These EPRI guidelines provide the technical information, project planning recommendations, and tools such as templates and checklists to assist responsible entities in the initial phases of reaching compliance with the NERC Cyber Security Reliability Standards (EPRI, 2006). Other related EPRI reports include: SCADA system security (2003); guidelines for detecting and mitigating cyber-attacks on electric power companies (2004); guidelines for securing control systems and corporate network interfaces (2005).

2006 - Roadmap to Secure Control Systems in the Energy Sector – This roadmap was a collaborative effort between government and industry owners and operators to identify steps and time-based milestones to secure control systems used in electricity, oil, and natural gas sectors over the following ten years. On the government side the work was a collaborative effort between DOE/OE, DHS/S&T, and the Energy Infrastructure Protection Division of Natural Resources Canada. The framework was designed to align program and investment strategies between industry and government. The roadmap focused on four key goals: measure and assess security posture; develop and integrate protective measures; detect intrusion and implement response strategies; and sustain security improvements. The roadmap defines control systems as "the facilities, systems, equipment, services, and diagnostics that provide the functional control capabilities necessary for the effective and reliable operation of the bulk energy system." While this standard includes mention of the supporting telecommunications infrastructure, the focus is

specific to security of the communication between remote access devices and control centers, security between business and control systems, and control system components with built-in, end-to-end security.

2007 - Energy Independence and Security Act (EISA) of 2007, Title XIII - The Energy Independence and Security Act (EISA) of 2007, Title XIII, established a national policy for grid modernization and provided incentives for stakeholders to invest in smart grid initiatives (EIA, 2011). At that time, Congress saw the need to leverage the ability to use digital and control technology to improve reliability, security and efficiency of electric grids. With an eye to the benefits of increased grid optimization and resulting efficiency improvements, Congress also realized that efforts would have to be made to secure these new networked systems from cyber vulnerabilities. While the Director of the National Institute of Standards and Technology was given the responsibility of developing protocols and standards to enable expansion of production and demand side technologies and systems, the Department of Energy was asked to assess the impacts of deploying smart grid systems. Three of the four focus areas for the DOE impacts study were recommendations related to positive benefits of smart grid. The fourth asked what risks needed to be taken into account and how those risks could be mitigated. (Government Printing Office, 2007). A portion of that report was produced in 2009 as part of the National SCADA Test Bed by Idaho National Laboratories (https://www.smartgrid.gov/files/Study_Security_Attributes_Smart_Grid_Systems_Current_Cyber_200903.pdf). It covers cyber vulnerabilities in the legacy systems of the power grid, smart grid technologies, smart grid deployment status, and a very brief discussion of smart grid security primarily related to the use of wireless networking by those technologies.

2009 - American Reinvestment and Recovery Act (ARRA) - The American Reinvestment and Recovery Act (ARRA) appropriated $4.5 billion for Title XIII projects and other efforts to modernize the grid (Keogh, 2009). For example, development of smart meters, distribution automation and demand response programs have been supported by the disbursement of almost $4.5 billion of ARRA funding (Energy Information Administration, 2011). Also, in their 2014 Smart Grid System Report to Congress, DOE notes that each recipient of SGIG funding under ARRA is required to develop a Cybersecurity Plan that ensures reasonable protections against broad-based, systemic failures from cyber breaches. DOE followed up with extensive guidance on plan implementation, annual site visits to the 99 recipients, and two workshops to exchange best practices (US Department of Energy, 2014).

2009 - DHS's National Cyber and Communication Integration Center (NCCIC) – The Department of Homeland Security set up NCCIC in 2009 to serve as a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations (DHS, 2016).

2009 - Federal Energy Regulatory Commission, Smart Grid Policy, 128 FERC ¶ 61,060 (2009) - Among their findings, the Commission identifies cyber security and communication and coordination as priorities across inter-system interfaces (Federal Energy Regulatory Commission, 2012).

2010 – NISTIR 7628 Guidelines for Smart Grid Cyber Security - In 2010, the Smart Grid Interoperability Panel Cyber Security Working Group published guidelines as an approach assessing cyber security issues and selecting and modifying cyber security requirements to address these issues. For the entire Smart Grid, the goal is to develop a cyber security strategy that effectively addresses prevention, detection, response, and recovery. The Guidelines are meant to be a flexible framework to be applied to securing the Smart Grid from an operational and technology development perspective (SGIP, 2010).

2011 - Roadmap to Achieve Energy Delivery Systems Cybersecurity – The 2011 roadmap was an update to the 2006 document. It included a broader focus on energy delivery systems, smart grid technologies, and the interface between cyber and physical security, new identified priorities and gaps, advancing threat capabilities, and emphasis on a security culture. While the new roadmap expands to smart grid technologies, it continues to focus on the bulk power system. Increasing use of distributed and alternative energy sources and increased reliance on the telecommunications industry and reliance on the Internet for communications are cited as drivers impacting future energy delivery systems security. The strategies and milestones in the roadmap do not seem to directly address these particular drivers and continue to focus on secure communications for the control system (such as the Secure SCADA Communications Protocol), among other goals. There is mention of cybersecurity and home area networks related to advanced metering infrastructure but the focus is accessibility and physical tampering (Energy Sector Control Systems Working Group, 2011).

2012 - Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline - In 2012, the U.S. Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and with input from members of industry and utility-specific trade groups, developed the electricity subsector cybersecurity RMP Guideline. This guideline is intended to help firms responsible for power generation, transmission, distribution, marketing, and supporting vendors apply effective and efficient risk management processes. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures (Edison Electric Institute, 2014) (US Department of Energy, 2012).

2012 - Electric Sector Cybersecurity Capabilities and Maturity Model (ES-C2M2) - In 2012, the electric power industry collaborated on a White House initiative led by DOE, in partnership with DHS, to develop the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to help measure and improve the industry's cyber readiness. The model helps electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity (Edison Electric Institute, 2014). In 2014, DOE released a second version (1.1) of the ES-C2M2, which uses a self-evaluation methodology to help grid operators assess their cybersecurity capabilities and prioritize actions and investments for improvement. To date, 104 utilities covering 69 million customers have downloaded the ES-C2M2 toolkit (US Department of Energy, 2014).

2013 - North American Electric Reliability Corporation (NERC), CIP V5 Transition Program - In November 2013, FERC approved Version 5 of the critical infrastructure protection cybersecurity standards (CIP Version 5) which represents significant progress in their efforts to protect the bulk power system against cybersecurity compromises and associated operational risks. In 2014, NERC initiated a program to help industry transition directly from the currently enforceable CIP Version 3 standards to CIP Version 5. The goal of the transition program is to improve industry's understanding of the technical security requirements for CIP Version 5, as well as the expectations for compliance and enforcement (NERC, 2015).

2014 - NIST issued Cybersecurity Framework Version 1.0 - In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity to offer a prioritized, flexible, repeatable, and cost-effective approach to manage cyber risk across the nation's critical sectors (i.e., financial, energy, health care, etc.). The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs. The framework allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. It is interesting to note that the framework document is labeled "Version 1.0" and is described as a "living" document that will need to be updated to keep pace with changes in technology, threats and other factors, and to incorporate lessons learned from its use (NIST, 2014) (US Department of Energy, 2014).

2016 – NERC CIPv6 – Implemented within FERC Order 822, NERC CIPv6 expands on prior iterations of the critical infrastructure protection cybersecurity standards. Key changes include the addition of requirements to address physical security located outside of physical security perimeters, where physical security is not in place. This translates into using other methods (encryption of data or logical controls) to deal with security concerns outside of physical security perimeters. Additionally, CIPv6 specifies the need for processes for authorization and mitigation of vulnerabilities, malicious code, and unauthorized use (Erlin, 2016).

State-Level Smart Grid Policies and Actions

Hawaii

2011 - Grid Enhancements Smart Grid Initiatives, Japan-U.S. Smart Grid project - Signed a memorandum of understanding with the Japanese government to build a first-of-its-kind smart grid demonstration project on the Island of Maui. The project is aimed at improving integration of variable renewable resources, such as solar and wind power, and preparing the electric system for widespread adoption of electric vehicles (NGA, 2015) (State of Hawaii, 2016).

2012 - Smart Grid Initiatives, Hawaii and Republic of Korea Sign Collaboration Agreement - Hawaii Governor Neil Abercrombie and Choi Kyu-Chong, the Republic of Korea's Director of the Electricity Market and Smart Grid Division at the Ministry of Knowledge Economy (MKE), have signed a letter of intent to pursue smart grid development in the Hawaiian Islands. The agreement forms the basis to collaborate on smart grid research, development and demonstration projects in conjunction with public/private partners from Korea, Hawaii and elsewhere in the United States (NGA, 2015) (State of Hawaii, 2016).

2012 - Electricity; Reliability Standards; Interconnection Requirements - Senate Bill 2787 **a**uthorized the Public Utilities Commission to: develop, adopt, monitor, and enforce electric reliability standards and interconnection requirements; contract for the services of a Hawaii Electricity Reliability Administrator to monitor and enforce standards, and perform other technical interconnection-related support functions; and establish procedures for interconnection on the Hawaii electric system and a surcharge to ensure the reliable operation of the Hawaii electricity system and overseeing of grid access on the system (NGA, 2015).

2013 - Power Grid Enhancements Smart Grid Initiatives, HI SB1040 – The purpose of the Act (enacted April 22, 2013) was to establish a policy for the State of Hawaii in support of implementation of advanced grid modernization technology. It authorized the Public Utilities Commission to consider the value of implementing advanced grid modernization technology, related to improvement of the operational capability of the electric system, automatic restoration of electrical service in response to power disturbance events, resilient operation against physical and cyber-based attacks, the ability to satisfy power quality requirements of new technologies and end users and accommodation of energy generation and storage choices (NGA, 2015).

2013 - State Energy Plans and Strategies - Hawaii Gov. Abercrombie and the Hawaii Energy Office unveiled a set of five policy directives to help spur the deployment of cost-effective energy resources to meet the state's clean energy and energy security goals. The two most relevant to this analysis is the goal to (1) diversifying the state's energy portfolio through the use of solar, wind, hydropower, and geothermal energy, along with liquefied natural gas as a transitional fuel, and, (2) modernizing the state's electric grid, which includes connecting some islands to promote system efficiency (NGA, 2015).

2014 - Reforming Utility Incentives for Clean Energy Comprehensive Reform, HB 1943 - Directs the Public Utilities Commission to work towards modernizing the electric grid. This action included several specific and related goals including: enabling a diverse portfolio of renewable energy resources, expanding customer options to manage their energy use, maximizing interconnection of distributed generation to the state's electric grid on a cost-effective basis at reasonable rates, determining fair compensation for electric grid services by distributed generation customers and maintaining grid reliability and safety through modernization of the state's electric grids, determining fair compensation for electric grid services and maintaining or enhancing grid reliability and safety through modernization of the state's electric grid (NGA, 2015).

2015 - Alternative Energy Portfolio Standards (§269-92, Renewable portfolio standards) - Over the past 10 years, Hawaii has steadily increased their alternative energy portfolio standards. The 2015 legislative action extended the RPS to 2045 and required 100% of electricity to come from renewable resources by that year, making Hawaii the first state in the nation to set a target of 100% renewable electricity. Technologies recognized in the RPS include: wind; solar thermal and photovoltaic (PV); geothermal; biogas including landfill methane; biomass including municipal solid wastes; hydroelectricity; seawater-chilled air conditioning; and wave, tidal, and ocean energy. State regulators also set separate energy efficiency portfolio standards, which are

aimed at reducing anticipated electricity consumption 30% by 2030 (EIA, State Profiles and Energy Estimates, 2016) (NGA, 2015).

California

2009 - Smart Grid Initiatives, SB 17 - Public Utilities Commission required to determine the requirements for a smart grid deployment plan consistent with the policies set forth in federal law.
Each electrical corporation required to develop and submit a smart grid deployment plan to the Commission (NGA, 2015) (CPUC, 2012).

2011 - California Public Utilities Commission, "Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System", Decision 11-07-056, July 28, 2011 - Create standards for data access and privacy that provide clear direction on customer data ownership and access. The three investor-owned utilities in the state are required to provide customers with daily information on their historic energy use and expected final monthly bill and develop plans to roll out home area network-enabled devices so that customers can access real-time data. Under the rules, customers have the sole right to authorize third parties to receive data, and utilities have no new liability for misuse of data by third parties. The CPUC will have jurisdiction over protecting data privacy when third parties get data from the utility but not over data accessed by third-party technologies directly from the customer's meter (NGA, 2014) (CPUC, 2012).

2015 – Los Angeles Department of Water and Power Smart Grid Regional Demonstration Program - LADWP is collaborating with a consortium of research institutions to develop new Smart Grid technologies, quantify costs and benefits, validate new models, and create prototypes to be adapted nationally. Among the goals of this program is Next-Generation Cyber Security: demonstrate technologies to show grid resilience against physical and cyber-attack, an operational testing approach for components & installed systems, and redefine the security perimeter to address Smart Grid technologies to the meter in residential and commercial sites (DOE, 2015).

2015 – Rule 21 Recommendations for the CPUC – The California Energy Commission and the CPUC drafted a series of cyber security and privacy requirements under Electric Rule 21, the tariff which describes interconnection, operation, and metering requirements for connection of generation facilities to the distribution system, as part of the Smart Inverter Working Group (SIWG), whose purpose is to mitigate the impact of high penetration of DERs.
Recommendations for cyber security under Phase 2 of the SIWG included a range of basic cyber security requirements (e.g., end-to-end requirements, implementation validation before data is exchanged, and a minimum of authentication, authorization, Accountability, and data integrity). Privacy policies are also to be clearly defined. A range of questions for utilities are posed to clarify inclusion in Rule 21. Existing confidentiality provisions can be used by utilities, such as privacy agreements between aggregators and their customers (CPUC, 2015).

2015 - Microgrid Development - San Diego Gas & Electric was awarded a nearly $5 million grant to support a 26-megawatt (MW) microgrid connected to a local solar facility. The microgrid will be connected to the energy grid but have the ability to disconnect during emergencies and supply solar electricity through onsite solar energy resources (SDG&E, 2015) (NGA, 2015).

Vermont

2011 - PSB Public Hearing No.7307, Investigation into Vermont Electric Utilities' Use of Smart Metering and Time-Based Rates - The PSB collected input from the public on issues related to smart meter data privacy and cybersecurity. The PSB also addressed the opt-out policy requiring a monthly fee if the customer chooses to retain the traditional electric meters (Energy Information Administration, 2011).

2012 - Wireless Smart Meters – Senate Bill 214 required the public service board to establish terms and conditions regarding wireless smart meters (NGA, 2015).

2014 - Net Metering Law - Requires separate interconnection standards for net-metered energy systems and for distributed-generation systems that are not net metered; requires electric utilities to offer net metering to all customers with photovoltaic systems, wind- energy systems, fuel cells or biomass-energy systems with limits (NGA, 2015).

2015 – Energy Portfolio Standards and Energy Efficiency - Vermont House Bill 40, passed into law June 11, 2015, raised the required amount of renewably sourced electricity that utilities must purchase to 55 percent of total purchases by 2017 and 75 percent by 2032 to spur the development of customer-sited energy resources such as home solar panels or wind turbines. Required that those sources provide 1 percent of the state's electricity by 2017 and 10 percent by 2032. Established a statewide OBR program through which utilities can provide customers with options to finance energy-efficiency improvements, including the ability to repay them through a discount on their monthly utility bill. Offered discounts through utilities on customers' monthly bills in exchange for energy efficiency home-improvements, with the utilities being repaid in the form of increased energy savings (NGA, 2015).

2016 – Vermont Comprehensive Energy Plan - The 2016 CEP embraces distributed energy concept in which a significant portion of Vermont's energy is produced near where it is consumed, and which is shaped by many coordinated actions by distributed energy users, rather than through singular central control. The underpinning of this vision is the increasing availability of cost-effective distributed electric generation technology, such as solar PV, along with the increasing opportunity to store electric and thermal energy, and the communications overlay that comes from near-universal broadband and smart grid deployment combined with "smart" appliances and other end-use energy control technologies. New power generation has come online from resources like wind and solar power that have no operating costs, are generally smaller in capacity, and are distributed in many locations around the distribution grid. The plan also sets targets to reduce total energy consumption per capita by 15% by 2025, and by more than one third by 2050. It sets a goal to meet 25% of the remaining energy need from renewable sources by 2025, 40% by 2035, and 90% by 2050 (DPS, 2016).

New York

2009 - New York State Smart Grid Consortium, 8/25/2009 - Governor's order establishing the New York State Smart Grid Consortium comprised of leaders from government, utility companies and universities, as well as consumers. Formed to develop a strategic vision on how best to deploy secure, efficient and reliable smart grid technologies in New York. Published report in 2009 indicating that all of New York's stimulus proposals submitted under the DOE smart grid funding solicitations complement one another (Energy Information Administration, 2011).

2011 - An Act to the Public Authorities Law, In Relation to Smart Grid Systems 1/11/2011 (AB 1656) - This bill would establish smart grid as the policy of the state, where smart grid systems will allow two-way digital communication between electric utilities, their distribution grid and customers. This would improve efficiency and reliability of the electrical distribution system while also decreasing electric prices throughout the state. Smart Grid Systems support homeland security concerns by providing increased protection of the state's electric grid. This system allows for remote monitoring of critical infrastructure and key assets which provides disaster prevention and recovery capabilities (Energy Information Administration, 2011).

2011 - Public Service Commission Takes Major Step Toward Modernizing the Grid, Framework Laid Out for Utilities to Create a Smarter Grid - Approved a policy statement that would establish regulatory policies and set forth guidelines for utilities to follow regarding the development of smart electric grid systems and associated efforts to modernize the electric grid (NGA, 2015).

2013 - Cybersecurity Initiative - As part of his 2013 State of the State address, New York Governor Andrew Cuomo launched a cybersecurity initiative that created a governor's Cybersecurity Advisory Board and called for the physical co-location of the state's intelligence center with the Multi-State Information Sharing and Analysis Center (MS-ISAC). That created a combined physical and cybersecurity operations center to more efficiently protect critical infrastructure networks, including energy systems.16 The operations center al- lows state and federal agencies to more easily share threat information and work cooperatively to address threats to critical infrastructure (NGA, 2014).

2014 - Power Grid Enhancements Transmission Planning and Siting - Governor Andrew Cuomo announced $4.3 million in state funding for a series of projects to improve reliability and operation of the electric power grid. Project examples include installing and testing advanced measurement units on transmission lines; testing advanced energy storage and microgrids; and launching a study into how large-scale, but intermittently generating, solar photovoltaic installations can be integrated into the electric power grid (NGA, 2015).

2014 - Resiliency Plans - Governor Andrew Cuomo unveiled the "Reimagining New York for a New Reality," a $17 billion strategy that is intended to transform New York's infrastructure, transportation networks, energy supply, coastal protection, weather warning system and

emergency management to better protect New Yorkers from future extreme weather events (NGA, 2015).

2015 - Reforming the Energy Vision – The New York Public Service Commission (PSC) identified a number of potential issues in a reformed electric system with utilities acting as Distributed System Platform (DSP) providers. Among the issues identified was security. The PSC recommended following the technical guidance for smart grid cyber security assembled by NIST as a primary reference, saying that "there is no single set of security standards that we can simply direct utilities to comply with. It is unlikely that any definitive set of standards will ever exist, given the threat." The PSC did not direct the adoption or development of a specific set of cyber security standards as part of this order (State of New York Public Service Commission, 2015).

2015 - Microgrid Development - Governor Cuomo announced the launch of the state's $40 million energy competition, NY Prize, which accepted proposals for microgrids that meet the energy and resiliency needs of local communities. The prize money for the winning designs will be used to build microgrids across New York (NGA, 2015).

2015 - Renewable/Alternative Energy Portfolio Standards - Governor Cuomo released the state's 2015 energy plan, which sets goals of 50 percent of electricity generated from renewable sources and a 40 percent reduction in GHG emissions (from 1990 levels) by 2030 (NGA, 2015).

2015 - Reforming Utility Incentives for Clean Energy Comprehensive Reform - Governor Cuomo announced new reforms to the state's energy and utility industry that will require the integration of energy efficiency, solar, wind, and other clean energy technologies into the grid to reduce energy bills and give customers greater control over their energy use. These developments are part of the governor's Reforming the Energy Vision plan (NGA, 2015).

State Level Renewable Energy Financial Incentive Examples

Hawaii

1998 - KIUC Solar Water Heating Rebate Program - Participants will receive an energy use analysis and screening for the installation of cost-effective energy saving devices, including solar water heating systems. Customers are eligible for a flat $1,000 rebate for each solar water heating system installed (NCCETC, 2016).

1998 - KIUC Solar Water Heating Loan Program - Through a partnership with Kauai Community Federal Credit Union (KCFCU) and Kauai County Housing Agency (KCHA), the Kauai Island Utility Cooperative (KIUC) provides qualifying members with zero-interest loans (5-year term) for solar water heating systems. The loan is available for installations of new systems, or to replace solar water heating systems that are over 15 years old and no longer work (NCCETC, 2016).

2001 - Hawaii Net-metering - Hawaii's original net-metering law was enacted in 2001. In October 2008, As part of the Hawaii Clean Energy Initiative, Hawaii's governor; the Hawaii Department of Business, Economic Development and Tourism; the Hawaii consumer advocate, and the HECO companies entered into an energy agreement that provides that there should be no system-wide caps on net metering, and that net metering should transition towards a feed-in-

tariff. In December 2008, the PUC issued an order to raise the aggregate capacity limit for net-metered systems in the service territories of HELCO and MECO. In January 2011, the PUC issued an order approving changes to Kauai's program, which was full, and the aggregate capacity limits for HECO companies were lifted and are now based on per-circuit caps rather than a percentage of peak demand. In October 12th, 2015 the Hawaii PUC voted to end net metering in favor of 3 alternative options: a grid supply option, a self-supply option, and a time of use tariff (NCCETC, 2016).

2002 - Maui Solar Roofs Initiative - Maui Electric Company (MECO) and the County of Maui teamed up to launch the Maui Solar Roofs Initiative to increase the use of renewable energy in Maui County. MECO administers the loan program and, through the Hawaii Energy Rebate Program, offers a $1,000 rebate for installations through its approved independent solar contractors (NCCETC, 2016).

2003 - City and County of Honolulu - Solar Loan Program - The Honolulu Solar Loan Program is offered by the City and County of Honolulu. The program offers zero-interest loans to income-eligible homeowners for the installation of solar water heating and photovoltaic systems through the City's Rehabilitation Loan Program (NCCETC, 2016).

2008 - Farm and Aquaculture Alternative Energy Loan - Hawaii enacted legislation (HB 2261) which created a loan program for agriculture and aquaculture renewable energy projects. Farmers and aquaculturists may receive loans for projects involving photovoltaic (PV) energy, hydroelectric power, wind power generation, methane generation, bio-diesel and ethanol production (NCCETC, 2016).

2009 - Feed-in-Tariff - Hawaii Public Utilities Commission (PUC) issued a decision that established a feed-in tariff in Hawaii. The feed-in tariff is offered by the three investor-owned utilities: HECO, MECO and HELCO. Several renewable energy technologies are eligible for the feed-in tariff, including solar photovoltaics (PV), concentrating solar power (CSP), on-shore wind and in-line hydropower. Under this program, qualified projects will receive a fixed rate over a 20-year contract. There are three tiers for rates, with the tiers and rates differentiated by technology and system size. The maximum caps on system size vary by island and by technology (NCCETC, 2016).

2009 - City and County of Honolulu - Real Property Tax Exemption for Alternative Energy Improvements - The Honolulu City Council unanimously passed Bill 58 to create a real property tax exemption for alternative energy improvements (alternative energy sources include solar, wind, hydropower, tidal, wave, solid waste and increased efficiency in fossil-fuel burning facilities). This bill became effective October 1, 2009. The alternative energy property installed on a building, property, or land is exempt from property taxes for 25 years (NCCETC, 2016).

2011 - GreenSun Hawaii - GreenSun Hawaii is a loan loss reserve fund developed using funds from the The American Recovery and Reinvestment Act of 2009 (ARRA). The GreenSun Hawaii program works with various lenders throughout Hawaii to offer financing for renewable energy and energy efficiency upgrades (NCCETC, 2016).

2012 - Solar and Wind Energy Credit - Originally enacted in 1976, the Hawaii Energy Tax Credits allow individuals or corporations to claim an income tax credit of 20% of the cost of equipment and installation of a wind system and 35% of the cost of equipment and installation of a solar thermal or photovoltaic (PV) system with variations depending on type of property (single family, multi-family, commercial) (NCCETC, 2016).

2013 - Green Infrastructure Bonds - Hawaii enacted legislation (SB 1087) allowing the Department of Business, Economic Development, and Tourism to issue Green Infrastructure Bonds to secure low-cost financing for clean energy installations, including both renewable energy and energy efficiency measures (NCCETC, 2016).

California

1975 - Santa Clara Water & Sewer - Solar Water Heating Program - The City of Santa Clara established the nation's first municipal solar utility. Under the Solar Water Heating Program, the Santa Clara Water & Sewer Utilities Department supplies, installs and maintains solar water heating systems for residents and businesses. Solar equipment is available from the city for heating swimming pools, process water and domestic hot water. The hardware (solar collectors, controls and storage tanks) is owned and maintained by the city under a rental agreement (NCCETC, 2016).

1999 - Property Tax Exclusion for Solar Energy Systems - Section 73 of the California Revenue and Taxation Code allows a property tax exclusion for certain types of solar energy systems installed between January 1, 1999, and December 31, 2016. Qualifying active solar energy systems include solar space conditioning systems, solar water heating systems, active solar energy systems, solar process heating systems, photovoltaic (PV) systems, and solar thermal electric systems, and solar mechanical energy (NCCETC, 2016).

1999 - City of Palo Alto Utilities - PV Partners (Rebate Program) - The City of Palo Alto Utilities (CPAU) PV Partners Program offers incentives to customers that install qualifying PV systems. The program, which has a budget of approximately $13 million over 10 years, is divided into 10 steps (residential incentives have 12 steps), each funded at $1.3 million (NCCETC, 2016).

2001 - Self-Generation Incentive Program - The Self-Generation Incentive Program (SGIP) offers incentives to customers who produce electricity with wind turbines, fuel cells, various forms of combined heat and power (CHP) and advanced energy storage (NCCETC, 2016).

2001 - Pasadena Water and Power - Solar Power Installation Rebate - Pasadena Water & Power (PWP) offers its electric customers a rebate for photovoltaic (PV) installations, with a goal of helping to fund the installation of 14 megawatts (MW) of solar power by 2017. As required by the California Solar Initiative, the PBI and EPBB incentive levels will step down annually over the 10-year life of this program (NCCETC, 2016).

2005 - Sacramento Municipal Utility District (SMUD) - PV Residential Retrofit Buy-Down - SMUD offers an incentive of $500 to residential customers who install grid-connected photovoltaic (PV) systems. The incentive will be adjusted based on expected system

performance, which is affected by factors such as inverter efficiency, orientation, tilt and shading (NCCETC, 2016).

2006 - California Solar Initiative, PV Incentive - The California Public Utilities Commission (CPUC) adopted the California Solar Initiative (CSI) to provide more than $2.3 billion in incentives for photovoltaic (PV) projects with the objective of adding 1,940 megawatts (MW) of solar capacity by 2016. The CSI is one element of the greater Go Solar California Campaign, which includes the New Solar Homes Partnership and the incentives offered by the Publicly Owned Utilities, and which has a total target of 3,000 MW of new solar capacity by 2016 (NCCETC, 2016).

2007 - Modesto Irrigation District - Photovoltaic Rebate Program - Modesto Irrigation District offers a photovoltaic rebate program for all of their electric customers. The peak output capacity of a system must be 1 kW or greater to participate. Systems up to 30 kilowatts (kW) in capacity can receive an up-front capacity-based incentive. Systems greater than 30 kW and up to 1,000 kW (1 MW) can receive a performance-based incentive. The rebate levels will decline over time (NCCETC, 2016).

2007 - LADWP - Solar Incentive Program (Rebate Program) - The California Solar Initiative, created in 2007 upon the enactment of SB 1, established new guidelines for municipal utilities to follow, and established new funding levels. The Solar Incentive Program has 10 phases with declining incentive levels as certain installed megawatt (MW) targets are met. LADWP's 10-year, $313 million Revised Solar Photovoltaic Rebate Program began in 2007 and will remain in effect through December 31, 2017, or until the total installed MW goal has been reached (NCCETC, 2016).

2007 - California Solar Initiative - Solar Thermal Program - AB 1470 of 2007 authorized the creation of a $350 million incentive program for solar water heating systems. Of the $350 million in total funding, $25 million is reserved for low-income incentives, $225 million is for systems that will displace natural gas water heaters, and $100 million is set aside for systems replacing electric water heaters. Originally restricted to just solar water heaters, the prorgam was expanded by CPUC Decision 13-02-018 in February 2013 to include other solar thermal technologies, including solar process heating, solar cooling, and non-residential solar pool heating. Similar to the PV incentives offered through the California Solar Initiative, the incentives offered through this program will step down four times as installation milestones are met. Steps will decline separately in each service territory and for the four general customer classes (NCCETC, 2016).

2007 - Silicon Valley Power - Solar Electric Buy Down Program - Silicon Valley Power (SVP) offers incentives for the installation of new grid-connected solar electric (photovoltaic, or PV) systems. Incentive levels will step down over the life of the program as certain installed capacity goals are met. As of May 2015, residential SVP customers are eligible for a rebate of $1.50 per watt AC up to $15,000 (10 kilowatts). Commercial SVP customers are eligible for a rebate of $0.90 per watt AC for systems up to 50 kilowatts (kW) (NCCETC, 2016).

2008 - Merced Irrigation District - PV Buydown Program - Merced Irrigation District (MID) offers its residential, commercial and non-profit customers a rebate for installing solar electric photovoltaic (PV) systems on their homes and offices. For 2015, the rebate is $1.00 per watt (adjusted based on the expected performance of the system) with a maximum of $3,000 for residential systems and $25,000 for non-residential systems (NCCETC, 2016).

2008 - California State-wide Property Assessed Clean Energy (PACE) Finance Program - PACE programs allow property owners to borrow money for energy improvement projects which are repaid through their property taxes. A number of energy efficiency and renewable energy technologies can be financed through FIGTREE's PACE program. FIGTREE Energy Financing is administering a Property Assessed Clean Energy (PACE) financing program in a number of California cities and counties through a partnership with the Pacific Housing & Finance Agency (PHFA) and the California Enterprise Development Authority (CEDA) (NCCETC, 2016).

2008 (latest update on net metering policy) - California Net Metering - The aggregate capacity limit of net-metered systems in a utility's service territory is equal to 5% of the utility's aggregate customer peak demand. Net excess generation (NEG) is carried forward to a customer's next bill. The renewable energy credits (RECs) associated with the electricity produced and used on-site remain with the customer-generator. If, however, the customer chooses to receive financial compensation for the NEG remaining after a 12-month period, the utility will be granted the RECs associated with just that surplus they purchase (NCCETC, 2016).

2010 - Marin Clean Energy - Feed-In Tariff - Assembly Bill 117, passed in 2002, allows communities in California to aggregate their load and to procure electricity from their own preferred sources. Under the authority of this law, California's first community choice aggregator, Marin Clean Energy (MCE), was launched in May of 2010. The Marin Energy Authority comprises each city and town in Marin as well as the communities of Belvedere, Fairfax, Mill Valley, San Anselmo, San Rafael, Sausalito, Tiburon, and the County of Marin (NCCETC, 2016).

2013 - LADWP - Feed-in Tariff (FiT) Program - LADWP is providing a Feed-in Tariff (FiT) program to support the development of renewable energy projects in its territory. All technologies eligible for compliance with the state's renewables portfolio standard are eligible for the FiT, though LADWP expects the majority of projects to be photovoltaic (PV) systems. The amount LADWP will pay for each kilowatt-hour (kWh) produced will be a product of the Base Price of Energy (BPE) multiplied by the appropriate Time-of-Delivery (TOD) Multiplier. The BPE is scheduled to decline as each 20 MW allocation is subscribed (NCCETC, 2016).

2012 - City of Palo Alto Utilities - Palo Alto CLEAN (Feed-In-Tariff) - City Palo Alto Utility's Clean Local Energy Accessible Now (CLEAN) program provides fixed payments for electricity produced by approved photovoltaic systems over a fixed period of time. This type of program is commonly referred to as a feed-in tariff. As of June 2015, the only option is a 20-year contract for a price of $0.165 per kilowatt-hour (kWh) (NCCETC, 2016).

2014 - Ukiah Utilities - PV Buy-down Program - Through Ukiah Utilities' PV Buy-down Program, residential and commercial customers are eligible for a $1.40-per-watt AC rebate on qualifying grid-connected PV systems up to a maximum system size of 1 MW. In keeping with SB1, the incentive level will decrease annually on July 1 over the 10-year life of the program. Rebates are available on a first come, first served basis and are limited to $7,000 per residential installation and $25,000 per commercial installation (NCCETC, 2016).

Vermont

1975 - Local Option - Property Tax Exemption - Vermont allows municipalities the option of offering an exemption from the municipal real and personal property taxes for certain renewable energy systems. Adoption of this exemption varies by municipality, but the exemption generally applies to the total value of the qualifying renewable energy system and can be applied to residential, commercial, and industrial real and personal property (NCCETC, 2016).

1998 - Vermont Net Metering - Vermont's original net metering legislation was enacted in 1998, and the law has been expanded several times, most recently by H.B. 702 of 2014. Any electric customer in Vermont may net meter after obtaining a Certificate of Public Good from the Vermont Public Service Board (PSB). Net metering is generally available to systems up to 500 kW in capacity that generate electricity using eligible renewable energy resources, including combined heat and power (CHP) systems that use biomass. Net metering is available on a first-come, first-served basis until the cumulative capacity of net-metered systems equals 15% of a utility's peak demand during 1996 or the peak demand during the most recent full calendar year, whichever is greater. Any customer net excess generation (NEG) is carried over to the customer's next bill. Any NEG shall be used within twelve months of the month earned; if not, it is granted to the utility with no compensation for the customer. Beginning January 1, 2017, the utility owns the renewable energy credits (RECs) generated by a customer's net-metered system, unless the customer elects not to transfer ownership of these RECs at the time of application. Until 2017, net-metered customers retain default ownership of RECs unless the customer elects to transfer ownership to the utility (NCCETC, 2016).

1999 - Renewable Energy Systems Sales Tax Exemption - Vermont's sales tax exemption for renewable energy systems, originally enacted as part of the Miscellaneous Tax Reduction Act of 1999 (H.B. 0548), initially applied only to net-metered systems. The exemption now generally applies to systems up to 500 kilowatts (kW) in capacity that generate electricity using eligible renewable energy resources, to micro-combined heat and power (CHP) systems up to 20 kW, and to solar water-heating systems. The exemption is available for grid-tied systems and off-grid systems alike (NCCETC, 2016).

2003 - Small-Scale Renewable Energy Incentive Program - Vermont's Small Scale Renewable Energy Incentive Program (SSREIP) currently provides funding for new solar water heating and advanced wood pellet heating installations. The program is available to single- and multi-family residences, commercial and industrial businesses, farms, schools, builders/developers, and local & state governments (NCCETC, 2016).

2004 - GMP Cow Power HVAC Equipment Rebate Program - Green Mountain Power Corporation (GMP), Vermont's largest electric utility, offers a production incentive to farmers

who own systems utilizing anaerobic digestion of agricultural products, byproducts, or wastes to generate electricity (NCCETC, 2016).

2008 - GMP Solar Power - Green Mountain Power, an investor-owned electric utility operating in Vermont, offers a credit to customers with net-metered photovoltaic (PV) systems. In addition to the benefits of net metering, Green Mountain Power customers with a PV system less than 15 kilowatts (kW) receive a credit of $0.053 per kilowatt-hour (kWh) of electricity generated by the system. PV installations larger than 15 kW receive a credit of $0.043 per kWh. This credit is available to all customers of Green Mountain Power. The incentive does not have a specified duration or expiration date (NCCETC, 2016).

2009 - Investment Tax Credit - Vermont offers an investment tax credit for installations of renewable energy equipment on business properties. The credit is equal to 24% of the "Vermont-property portion" of the federal business energy tax credit. For solar, small wind, and fuel cells this constitutes a 7.2% state-level credit for systems placed in service on or before 12/31/2016. After this date, solar (except hybrid solar lighting) technologies are eligible for a 2.4% credit. For microturbines, and combined heat and power systems, the credit is a 2.4% state-level tax credit for systems place in service on or before 12/31/2016 (NCCETC, 2016).

2009 - Standard Offer Program (Feed-In-Tariff) - Vermont enacted legislation requiring all Vermont retail electricity providers to purchase electricity generated by eligible renewable energy facilities through the Sustainably Priced Energy Enterprise Development (SPEED) Program via long-term contracts with fixed standard offer rates. This policy, commonly known as a "feed-in tariff", is intended to provide a reasonable return on investment to renewable energy facility developers, thereby spurring deployment of renewable energy (NCCETC, 2016).

2013 - Uniform Capacity Tax and Exemption for Solar - Vermont fully exempts solar photovoltaic (PV) systems up to 50 kilowatts (kW) from the statewide education property tax. For systems 50 kW and greater, the state assesses a uniform tax of $4.00 per kilowatt (kW) in lieu of the statewide education property tax. A system up to 50 kW that is net-metered OR is not connected to the grid and only provides power to the property on which it is located is also exempt from municipal property taxes. A system up to 50 kW that is not net-metered and is connected to the grid OR is not connected to the grid but provides power to multiple properties is subject to municipal property taxes, unless the municipality has created a local exemption. Systems 50 kW and greater that are net-metered may reduce their capacity by 50 kW for valuation purposes if they are subject to municipal property taxes (NCCETC, 2016).

2013 - Small Business Energy Loan Program - The Small Business Energy Loan Program (SBELP) provides loans to businesses for smaller renewable energy and energy efficiency projects (NCCETC, 2016).

2013 - Commercial Energy Loan Program - The Commercial Energy Loan Program (CELP) provides loans to businesses for larger renewable energy and energy efficiency projects (NCCETC, 2016).

2013 - Agricultural Energy Loan Program - The Agricultural Energy Loan Program (AELP) provides loans to agriculture- or forest product-based companies for renewable energy and energy efficiency projects (NCCETC, 2016).

New York

1997 - New York Net Metering - Net metering is available on a first-come, first-served basis to customers of the state's major investor-owned utilities, subject to technology, system size and aggregate capacity limitations. New York's original net-metering law, enacted in 1997, applied only to residential photovoltaic (PV) systems up to 10 kilowatts (kW). In 2002, the law was expanded (S.B. 6592) to include farm-based biogas systems of up to 400 kW (increased to 500 kW in 2008) that generate electricity from biogas produced by the anaerobic digestion of agricultural waste, such as livestock manure, farming waste and food-processing wastes. In 2004, S.B 4890-E (of 2003) further expanded the law to include residential wind turbines up to 25 kW and farm-based wind turbines up to 125 kW. In August 2008 New York enacted a series of bills (S.B. 7171, S.B. 8415, and S.B. 8481) again amending the state's net metering laws, most notably extending net metering eligibility to non-residential PV and wind systems. In February 2009 the New York Public Service Commission (PSC) issued an order revising and approving several utility tariffs associated with these changes. A second order issued in June 2009 addressed further tariff filings and ordered changes to these and some previously filed tariffs. In August 2009 A.B. 2442 amended the law yet again to allow net metering for residential combined heat and power (CHP) and fuel cell systems of 10 kW or less, with utility tariffs approved in February 2010. Further legislation (A.B. 7987) enacted in August 2010 increased the capacity limit for farm-based biogas systems from 500 kW to 1 MW and revised tariffs were approved in December 2010. For most types of systems, customer net excess generation (NEG) in a given month is credited to the customer's next bill at the utility's retail rate. A slightly different methodology using a monetary credit ($ as opposed to kWh) is used for customers on demand meters. At the end of each annual billing cycle, most customers (i.e., residential PV and wind and farm-based wind and biogas systems) will be paid at the utility's avoided-cost rate for any unused NEG. Compensation for unused NEG produced by non-residential wind and solar systems is not addressed by the statute, however, the New York Public Service Commission (PSC) determined in its February 2009 order that unused NEG for such systems should be carried forward from one year to the next. Likewise, residential micro-CHP and fuel cell customer-generators are not permitted to monetize NEG after a year or any other period, but may carry forward unused credits indefinitely. Recently enacted S.B. 1149 did not identify a specific annual reconciliation protocol for micro-hydroelectric facilities, but the recently approved utility tariffs provide for indefinite carryover (NCCETC, 2016).

1997 - Residential Solar Tax Credit - Enacted in August 1997, this personal income tax credit originally applied to expenditures on solar-electric (PV) equipment used on residential property (NCCETC, 2016).

2005 - New York City - Residential Solar Sales Tax Exemption - In July 2005, New York enacted legislation that allows local governments to grant a local sales tax exemption for residential solar energy systems. New York City passed Resolution 1121 in August 2005 to exempt residential solar energy systems equipment and services from sales tax (NCCETC, 2016).

2005(Residential), 2013(Commercial) - Local Option - Solar Sales Tax Exemption - New York enacted legislation in July 2005 exempting the sale and installation of residential solar-energy systems from the state's sales and compensating use taxes. The exemption applies to solar-energy systems that utilize solar radiation to produce energy designed to provide heating, cooling, hot water and/or electricity. In 2012 the exemption was also extended to commercial solar energy systems, effective January 1, 2013. In 2015 the exemption was extended to solar systems that are owned by third party owners, who provide solar electricity to residential and commercial users. Both solar lease payments and the receipts of the sale of electricity by such systems are exempt from state sales and use tax (NCCETC, 2016).

2008 - New York City - Property Tax Abatement for Photovoltaic (PV) Equipment Expenditures - In August 2008 the State of New York enacted legislation allowing a property tax abatement for photovoltaic (PV) system expenditures made on buildings located in cities with a population of 1 million or more people (NCCETC, 2016).

2009 - NY-Sun Loan Program - NY-Sun loan program is part of broader NY-Sun Initiative program to accelerate the use of solar PV across the State. In addition to cash incentives, NY-Sun Initiative also provides State sponsored low-interest financing options to install solar PV systems (NCCETC, 2016).

2010 - NY-Sun PV Incentive Program (Residential, Low-Income, and Small Business) -The New York State Energy Research and Development Authority (NYSERDA) through NY Sun Incentive Program (PON 2112) provides cash incentives for the installation of approved, grid-connected photovoltaic (PV) systems. The program was re-launched in 2014 with a goal of supporting 3.175 GW of installed capacity by 2023. The program provides cash incentives for residential solar systems that are 25 kW or less, and for non-residential systems that are 200kW or less. NY-Sun solar incentives are designed to phase out in a controlled and predictable manner over time depending on installed solar capacity in the given region (NCCETC, 2016).

2010 - Solar Thermal Incentive Program - The New York State Energy Research and Development Authority (NYSERDA) offers incentives for the installation of solar water heating systems for residential, commercial, agricultural, governmental, and not-for-profit institutional customers of the state's major investor-owned utilities. The program is part of the Customer-Sited Tier (CST) of the state renewable portfolio standard (RPS) (NCCETC, 2016).

2012 - On-Site Wind Incentive Program -The New York State Energy Research and Development Authority (NYSERDA) provides incentives for eligible small wind systems. Incentive payments are paid directly to the eligible installers, who pass on the savings to the customers (NCCETC, 2016).

2013 - PSEG Long Island - Solar Initiative Feed-in Tariff - The PSEG Long Island Feed-in Tariff II (FIT II) program provides fixed payments for electricity produced by approved photovoltaic systems over a fixed period of time. The program operates under a sell-all arrangement, where the full amount of energy production from the facility is sold to the utility (i.e., no on-site use). The program offers a 20-year contract at a rate determined through the

Clearing Price Auction. A total of up to 100 MW of new solar generation will be supported by the FIT II program. The system size is determined as the lesser of the sum of the AC rated output of all inverters, or the PTC rating of the system multiplied by the inverter efficiency. Projects must be connected to the LIPA grid at the distribution level, defined as 13.2 kilovolts (kV) or below (NCCETC, 2016).

2013 - NY Green Bank - In December 19, 2013 the Public Service Commission (PSC) approved a petition issued by NYSERDA's to establish and fund the operations of New York Green Bank (NY Green Bank). NY Green Bank is a state-sponsored specialized financial entity, working to accelerate clean energy deployment throughout New York State by partnering with the private sector to address and alleviate market and financial barriers preventing a thriving clean energy marketplace. NY Green Bank does not accept deposits or offer retail loans, and instead works on the wholesale level, operating in direct response to real-time market needs (NCCETC, 2016).

2014 - Local Option - Solar, Wind & Biomass Energy Systems Exemption - Section 487 of the New York State Real Property Tax Law provides a 15-year real property tax exemption for solar, wind energy, and farm-waste energy systems constructed in New York State. As currently effective, the law is a local option exemption, meaning that local governments are permitted decide whether or not to allow it. The exemption is valid unless a government opts out of the exemption, as opposed to the more common practice of requiring governments to "opt-in" in order to offer an exemption. As originally created, the exemption was limited to solar and wind energy systems, but in September 2002, it was expanded to include farm-waste energy systems (NCCETC, 2016).

2015 - NY-Sun Commercial/Industrial Incentive Program - New York State Energy Research and Development Authority (NYSERDA) through NY-Sun Commercial/Industrial Incentive Program (PON 3082) provides incentives for installation of non-residential new grid connected solar photovoltaic (PV) systems that are greater than 200 kW. Incentives for systems smaller than 200 kW systems are offered through the NY-Sun PV incentive program. Incentives are awarded on a first-come, first serve basis, until the funds are fully committed. Applications are being accepted through December 29, 2023 (NCCETC, 2016).

1 Raisa Ledesma
U.S. Department of Energy
Office of Energy Policy and Systems Analysis
1000 Independence Ave. SW
Washington, DC 20585

1	MS0671	Jordan M. Henry	5628
1	MS0671	Jason E. Stamp	5623
1	MS0750	Lori K. Parrott	6913
1	MS1104	Charles J. Hanley	6110
1	MS1137	Kevin L. Stamber	6132
1	MS1137	Andjelka Kelic	6921
1	MS1137	Robert A. Taylor	6921
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories